UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/749,558	01/02/2004	Hsiang-Tsung Kung	6720.0110-01	8770

22852 7590 01/28/2009

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
TRAN, ELLEN C	
ART UNIT	PAPER NUMBER
2434	

MAIL DATE	DELIVERY MODE
01/28/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Advisory Action Before the Filing of an Appeal Brief	Application No.	Applicant(s)	
	10/749,558	KUNG, HSIANG-TSUNG	
	Examiner	Art Unit	
	ELLEN TRAN	2434	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 09 January 2009 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☐ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

a) ☒ The period for reply expires *4* months from the mailing date of the final rejection.

b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).

5. ☐ Applicant's reply has overcome the following rejection(s): _____.

6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: *1,3-38 and 40-81*.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).

9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).

10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.

12. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____

13. ☐ Other: _____.

/ELLEN TRAN/
Primary Examiner, Art Unit 2434

Continuation of 11. does NOT place the application in condition for allowance because: No argument was presented of amendment to the claims made that overcome the Final Rejection mailed 9 September 2008.

In response to Applicant's argument beginning on page 3, "In particular, with regard to the rejection of independent claims 1 and 38 as unpatentable over Murphy et al. and Ishibashi et al., Applicant pointed out that Murphy et al. fails to teach or suggest at least a PAD comprising "at least one storage medium storing at least one CA public key …[and] a processing component for authenticating one or more received digital certificates using the at least one stored CA public key".

The Examiner disagrees with argument, and notes that the references must be considered for all they teach and suggest. Murphy teaches in col. 5, lines 52-65 that the smart card stores public and private RSA cryptographic key pairs as well as that the CA distributes the smartcard as well as the information on the smartcard is provided by the CA, therefore the smartcard stores a CA public key. Second Murphy teaches that the smart card provided by the CA also stores certificates that are also provided by the CA. It is known in the art a certificate coming from a CA is authentic. In addition Murphy teaches that the smartcard has an on-board math co-processor that performs the key generation and encryption/decryption calculation, Obviously one of these calculations could be to insure that the certificate from the CA is actually from the CA, i.e. that the digital signature matches the expected based on the CA public key.

In response to Applicant's continued arguments that the smartcard does not store a public key of a CA and that Murphy does not require the use of the public key of the CA. The Examiner points to the following which is known in the art about certificates.

Structure of a certificate
The structure of an X.509 v3 digital certificate is as follows:

- Certificate
- Version
- Serial Number
- Algorithm ID
- Issuer
- Validity
  - Not Before
  - Not After
- Subject
- Subject Public Key Info
  - Public Key Algorithm
  - Subject Public Key
- Issuer Unique Identifier (Optional)
- Subject Unique Identifier (Optional)
- Extensions (Optional)
- Certificate Signature Algorithm
- Certificate Signature.

As stated above when a CA issues a certificate it contains the information needed to authenticate the certificate. In addition Murphy teaches that public keys are provided on the smartcard along with a co-processor that can be used for encryption/decryption operations. These operations would include authenticating a certificate issued by a CA. This form of authentication is commonly done by comparing the signature on the certificate.

In addition as support for the Examiner's response the Murphy references teaches in col. 7, lines 22-29, that although the example provided is for authenticating the user's social security number … any type of data could be stored or retrieved from the smart card, such as tickets, certificates, public/private keys, and so forth.